Specialized Technical Services

Prepared for

eGovernment Portal

Introduction

This document is intended to provide a high level description of the recommendation and justifications for the architecture expansion and update in order to accommodate for the portal and to build a scalable foundation to for future E-Government Projects and Services.

With the introduction of the portal and the FileNet components to the E-Government data center, Security becomes a more pressing issue in order to accommodate for G-to-C activities via the internet and to facilitate a secure access to the ministries that are not currently part of the SGN to manage their portal contents. This second requirement and due to the nature of FileNet CM engine will require allowing external users the access to internal systems.

As a result the need for tight and reliable security becomes immediate since inadequate information security creates a substantial risk that threatens not only important organizational assets, but also business processes critical to the continued operation of the organization itself. Like other insurance schemes, information security measures are in the end ways of protecting the business of The E-Government Data Center from a growing list of potential threats.

In this document the new items that we recommend to be introduced to the architecture in order to achieve satisfactory levels of security and information integrity are described.

Two-Levels Firewalls Security Architecture

Since the SGN is currently being expanded to accommodate for external users from other ministries in addition to housing the portal. A single line of defense for the network is no longer sufficient for the following reasons:

- Allowing external users access will enforce the relaxation of some of the security rules on the firewall.
- Introducing web services to the network creates the need to ensure that traffic between the Internet and the server does not traverse any part of your private internal network and that no internal network traffic is visible to the server.

Why this is important

A public Web server host is a computer intended for public access. This means that there will be many people who will access the host (and its stored information) from locations all over the world. Regardless of how well the host computer and its application software are configured, there is always the chance that someone will discover a new vulnerability, exploit it, and gain unauthorized access to the Web server host (e.g., via a user account or a privileged account on a host with a multiuser operating system). If that occurs, you need to prevent these subsequent events, if possible:

- The intruder is able to observe or capture network traffic that is flowing between internal hosts. Such traffic might include authentication information, proprietary business information, personnel data, and many other kinds of sensitive data.
- The intruder is able to get to internal hosts, or to obtain detailed information about them.

Therefore A second line of defense behind the web server is a requirement.

Second set of firewalls is needed and this can be done in two ways:

1. Using same brand firewalls as in the frontlines but configured with tighter security rules.
    - **Advantage:** Less management overhead and admin training requirements.
    - **Disadvantage:** If the first line firewalls firmware was exploited by default the second will also be exploited.

2. Or deploying a different brand of firewall also configured with a tighter set of security rules
    - **Advantage:** Hackers succeeding in penetrating the first line of defense will not automatically gain access to the internal instead they will be faced with yet another challenge.
    - **Disadvantage:** Extra Administration overhead.

If different brand firewall are to be used and since Cisco Pix is already chosen we recommend that the additional set of firewalls to be based on a software base firewall since the batches and bug fixes are issued faster for software base systems than the firmware revisions for the hardware firewalls.

Our Recommendation goes to either:

- SunScreen SecureNet
- Or Checkpoint Firewall-1

Recommendations are based on our knowledge and experience with both products.

Hardened Web Operating Environment

It is our recommendation to harden the web environment for two main reasons:

1. The web servers carrying the portal HTML pages will reside behind the first set of firewalls which creates the need for a second set of security measure.

2. Portal contents are published to static HTML, that will rely solely on the Operating System Security. This scenario increases the attack risk even for users legitimately passing through the firewall since there are numerous exploit information available on the Internet and it does not take a lot of skill to obtain an appropriate exploit to attack a server. In other words, any users passes through firewall will landing on some internal server, therefore this server has to be secure in and of itself.

A Hardened/Trusted Operating Environment provides methods for limiting *external* access, as well as extensive *internal* protection against intruders and misuse as follows:

- ***Limiting access to system data and resources.*** Hardened/Trusted Operating Environment allows controls to be set on all potential interactions with its programs, utilities, and file access. Both identity-based and label-based policies are enforced, which means users get the access and functionality they need, while at the same time the system is protected from unauthorized use.

- ***Eliminating superuser.*** Superuser functions are divided into multiple roles, making it far more difficult for compromising key individuals to penetrate the network. Provided that the Trusted / Hardened Operating Environment is configured properly it won't matter if a user has the root password since root has no privileges he has not power to do anything that could harm the system. Even if someone writes a buffer overflow for a program, it doesn't matter since root has no power to execute the malicious code

- ***Preventing "eavesdropping".*** In conventional environments, an intruding program can capture keystrokes typed in other windows. Hardened/Trusted Operating Environment provides a "trusted" path that protects entered data, which is particularly important for protecting passwords.

- ***Security auditing.*** Actions that may affect security or sensitive files can be monitored.

- ***Community Separation:*** Typical requirements for the setup at hand is for content developers from the ministries to be able to update their content via the internet, without being able to interfere with other ministries data or the operating system. One solution is to give each ministry its own dedicated host which is impractical. With hardened / Trusted Operating environments it is possible to enforce these security measures.

Platform

There are several products available for OS hardening however based on:

- The requirements specified above
- Our experience
- The adoption ratio in the international and regional markets

We are recommending either of the following two products:

- Argus Pitbull
- Sun Microsystems Trusted Solaris.

Also available commercially from HP "VirtualVault" but it was not recommended for the following reasons:

- Difficulty of Configurability
- Compartmentalization is limited
- Less mature integration tools than the recommended products.
- It has no privilege hierarchy.

Argus Supported web servers:
Argus supports a large number of products and platforms Complete listing is available at this URL: http://www.argus-systems.com/public/docs/support_applications.pdf

Trusted Solaris Supported web servers:
Trusted Solaris works with any web server that supports the Solaris operating environment, but it will require some additional configuration. Complete listing is available at this URL: http://sdc.sun.com/solaris8/s8supported_prod_alpha.html

In addition some companies developed web packages that utilizes the features of Trusted Solaris.

Trusted Web Server **by Trusted Systems Laboratories.** 303 Almaden Blvd., Suite 600 San Jose, CA 95110 Telephone: 408-938-5770 Facsimile: 408-938-5771 e-mail: sales@TrustedSysLabs.com Website: www.TrustedSysLabs.com	**Trusted Web Server** **By DigiGAN** 285 Hunting Ridge Road Stamford, CT 06903 Phone: 203.968.0441 Fax: 203.968.1707 Email: info@digigan.com Website: www.digigan.com

Budgetary figures

Argus Pitbull

Sadek, I could not figure out the pricing scheme so we need to consult with B1 for this part

Part No.	***Description***	***Budgetary Unit Price USD***	***Qty***	***Total***

Trusted Solaris

Part No.	***Description***	***Budgetary Unit Price USD***	***Qty***	***Total***
TS8IS-080-W999	TSol8 4/01, Wrkgp, Kit & RTU, SPARC	11,900.00	2	23,800.00

Hardware.

The commercially available Hardening systems are available for the UNIX/RISC platform as follows:

- Trusted Solaris is available for the Solaris SPARC platform
- Argus is available for Solaris, AIX and Linux. However the .Com components for the web is only available for Solaris and AIX

Hence, we are recommending the following hardware sizing measures based on RISC/Unix architectures for the required web servers [G-to-G or G-to-C] and for the search engine if the chosen search engine supports Unix.

General Hardware Sizing Requirement

3. Starting with 2 CPU’s minimum and expandable to at least 4
4. Starting with 4GB RAM and expandable to at least 16GB RAM
5. Starting with 2 x 36GB Hard Disks with the ability to expand internally or externally.
6. Minimum 2 Gigabit Ethernet interfaces
7. Rack-able.
8. Supports remote Management.

Based on the recommended Hardening products following are the hardware servers that comply with the previous specifications and supported by the Hardening products

Compliant Servers

- Sun Fire V480 [Argus & Trusted Solaris]
- IBM 430 [Argus]

Following are budgetary figures for a Single Sun 480 server.

Par Number	***Description***	***Qty***	***Budgetary Unit Price in USD***
A37-WSPF2-04GQB	SFV480:2@900MHz Cu,4GB,2-36 GB, DVD, 2 10/100/1000 ethernet	1	$27,625.00
X3768A	PGX64 CARD W/VIDEO ADAPTOR	1	$493.00
SOLZS-08HB9AYM	S8 2/02 SA kit CD/DVD, Eng doc	1	$111.00
X3538A	US UNIX/UNIX UNIV./EUR.UNIX	1	$57.00
X7143A	17" Entry Color Monitor	1	$357.00
X311L	NORTH AMERICAN/ASIA PWR CRD KT	1	$0.00

Optional Item Sun Microsystems Cabinet.

Par Number	***Description***	***Qty***	***Budgetary Unit Price in USD***
SG-XARY030A	72" STOREDGE EXPANSION RACK	1	$9,010.00
X9818A	Optional Front Door	1	$ 816.00

Cabinet can hold up to 6 sun fire v480 servers.